AMENDMENTS to the CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A system for authenticating a client device requesting a session of service from a service provider, comprising:

a first one-time pad cryptological table accessible by a cellular telephone service security server, said first table having multiple sequenced entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each entry containing at least one One Time Pad value;

a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

a code transmitter portion of said authentic cellular telephone device configured to select an unused entry in said second one-time pad cryptological table, and to transmit said selected entry to a telephone network upon requesting initiation of a service session;

a code exchanger portion of said cellular telephone service security server configured to receive a One Time Pad value from said authentic cellular telephone device and from said cloned inauthentic cellular telephone device upon request for initiation of a service session;

a code comparator portion of said cellular telephone service security server configured to determine that said received One Time Pad value [[is]] matches a sequentially next entry marked ~~as "used" or~~ "unused" in said first one-time pad cryptological table;

a service session grantor configured to grant said service request responsive to determination that said received One Time Pad value [[is]] matches a sequentially next unused entry, including changing said used indicator to a "used" state in said first one-time pad cryptological table upon said grant of service, and further configured to disable service to said cloned inauthentic cellular telephone device responsive to determining that said first one-time pad cryptological table is not synchronized with said first copy of said second

one-time pad cryptological table; and

a table updater portion of said authentic cellular telephone device configured to, responsive to granting of said service request, mark said transmitted One Time Pad as "used", wherein said first one-time pad crytological table and said second one-time pad cryptological tables are kept in synchronization.

2. (previously presented) The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise a sequence index;

said code comparator is further configured to determine if said received One Time Pad value is a next unused pad according to said sequence indicators; and

said session grantor is configured to grant a session only if said received pad is a next expected One Time Pad value.

Claims 3 - 4 (cancelled).

5. (previously presented) The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise an expiration field for each entry;

said code comparator is further configured to determine if said received pad is expired;

said session grantor is configured to grant a session only if said received pad is unexpired; and

said client device reconfigurator is configured to respond to said received pad being expired.

6. (cancelled)

7. (previously presented) The system as set forth in Claim 1 wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".

8. (currently amended) A method for authenticating a client device requesting a session of service from a service provider, said method comprising ~~the steps of~~:

providing a first one-time pad cryptological table accessible by a cellular telephone service security server, said table having multiple sequenced entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each entry containing at least one One Time Pad value;

providing a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

providing a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

selecting by a portion of said authentic cellular telephone device an unused entry in said second one-time pad cryptological table, and transmitting said selected entry to a telephone network upon requesting initiation of a service session;

receiving by a portion of said cellular telephone service security server a One Time Pad value from said authentic cellular telephone device or from said inauthentic clone cellular telephone device;

determining by a portion of said cellular telephone service security server if said received One Time Pad value [[is]] matches a sequentially next entry marked as ~~"used" or~~ "unused" in said first one-time pad cryptological table;

responsive to determination that said received One Time Pad value [[is]] matches a sequentially next unused entry, granting said service request and changing said used indicator corresponding to said One Time Pad entry in said first one-time pad cryptological table to a "used" state; and

responsive to determining that said received One Time Pad value is marked as "used" in said first one-time pad cryptological table, disabling service to said cloned inauthentic cellular telephone device wherein authentication of said authentic cellular telephone device is completed without need for a service history counter.

9. (previously presented) The method as set forth in Claim 8 wherein:

said one-time pad cryptological tables further comprise providing a sequence index field for each table entry;

determining that said received One Time Pad value is used comprises determining that said received One Time Pad is a next unused One Time Pad value according to said sequence indicators;

said granting comprises granting a session responsive to said received One Time Pad value being a next expected pad value.

10. (cancelled)

11. (previously presented) The method as set forth in Claim 9 wherein said challenging a user comprises challenging a user with one or more methods selected from a group comprising requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

12. (previously presented) The method as set forth in Claim 8 wherein:

providing one-time pad cryptological tables further comprises providing an expiration field for each entry;

determining that said received One Time Pad comprises determining that said received One Time Pad is expired;

granting a session comprises granting a session only responsive to said received One Time Pad is unexpired; and

challenging a user and replacing said tables comprises challenging a user responsive to said received pad being determined to be expired.

Claims 13 - 14. (cancelled)

15. (previously presented) An article of manufacture for authenticating a client device requesting a session of service from a service provider, comprising:

a computer readable medium suitable for encoding one or more software programs; and

one or more software programs configured to cause a processor to perform the steps of:

providing a first one-time pad cryptological table accessible by a cellular telephone service security server, said table having multiple sequenced entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each entry containing at least one One Time Pad value;

providing a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

providing a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

selecting by a portion of said authentic cellular telephone device an unused entry in said second one-time pad cryptological table, and transmitting said selected entry to a telephone network upon requesting initiation of a service session;

receiving by a portion of said cellular telephone service security server a One Time Pad value from said authentic cellular telephone device or from said inauthentic clone cellular telephone device;

determining by a portion of said cellular telephone service security server if said received One Time Pad value [[is]] matches a sequentially next entry marked as ~~"used" or~~ "unused" in said first one-time pad cryptological table;

responsive to determination that said received One Time Pad value [[is]] matches a sequentially next unused entry, granting said service request and changing said used indicator corresponding to said One Time Pad entry in said first one-time pad cryptological table to a "used" state; and

responsive to determining that said received One Time Pad value is marked as

"used" in said first one-time pad cryptological table, disabling service to said cloned inauthentic cellular telephone device wherein authentication of said authentic cellular telephone device is completed without need for a service history counter.

16. (previously presented) The article as set forth in Claim 15 wherein:
said software for providing one-time pad cryptological tables further comprises software configured to provide a sequence index field for each table entry;
said software for determining that said received One Time Pad value is used comprises software configured to determine that said received pad is a next unused pad value according to said sequence indicators; and
said software for granting a session comprises software configured to grant a session only responsive to said received pad value being a next expected pad value.

Claim 17 (cancelled).

18. (previously presented) The article as set forth in Claim 15 further comprising software configured to challenge a user with one or more methods selected from a group comprising requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

19. (previously presented) The article as set forth in Claim 15 wherein:
said software for providing one-time pad cryptological tables further comprises software configured to provide an expiration field for each entry;
said software for determining that said received One Time Pad comprises software configured to determine that said received One Time Pad is expired;
said software for granting a session comprises software configured to grant session only responsive to said received One Time Pad being unexpired; and
said software for challenging a user and replacing said tables comprises software configured to challenge a user responsive to said received One Time Pad being determined to be expired.

Claims 20 - 21 (cancelled)